Opinnäytetyö (AMK)

Tietojenkäsittely

2019

Aki-Petteri Koskela

JATKUVAN TUNNISTAUTUMISEN JÄRJESTELMÄN SUUNNITELMA

ääniohjatulle työnohjausjärjestelmälle

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2019 | 16 sivua

Aki-Petteri Koskela

JATKUVAN TUNNISTAUTUMISEN JÄRJESTELMÄN SUUNNITELMA

ääniohjatulle työnohjausjärjestelmälle

Työn toimeksiantaja yrityksellä on ääniohjattava työnohjausjärjestelmä, johon on tarpeena kehittää tunnistautumisjärjestelmä. Tarkoituksena kehittää ohjelmiston luotettavuutta ja varmuutta laadunvarmistuksessa. Tämän työn tarkoituksena oli luoda suunnitelma tunnistautumisjärjestelmän arkkitehtuurille sekä valita teknologiat, joilla sen voi toteuttaa. Käytännön osuudessa toteutettiin mahdollisimman suuri osa suunnitelmasta.

Suunnitelman toteuttaminen tapahtui tekemällä töitä yrityksen ohjelmiston parissa. Tarkoituksena oli saada ymmärrys ohjelmiston toiminnasta sekä yrityksen tarpeista. Nopeasti tuli esille, että yrityksen tarpeisiin sopii moniosainen biometrinen tunnistautumisjärjestelmä. Valitut biometriset tunnistautumiskeinot ovat kasvontunnistus ja äänen biometria. Niiden lisäksi valittiin myös PIN-koodi lisätunnistautumista varten. Järjestelmä suunniteltiin modulaariseksi, siten että uusia tunnistautumisteknologioita ja -innovaatioita pystyy tarvittaessa ottamaan käyttöön mahdollisimman helposti.

Käytännön osuudessa ehdittiin toteuttamaan valmis suunnitelma tunnistautumisjärjestelmän kokonaisarkkitehtuurista, joka sisältää valitut menetelmät ja teknologiat, jotka sopisivat yrityksen tämänhetkisiin tarpeisiin. Lisäksi käytännön osuudessa ehdittiin toteuttamaan kasvojentunnistus sekä PIN-koodi toiminnot. Kehitystyötä tullaan jatkamaan tähän suunnitelmaan perustuen.

ASIASANAT:

Biometria, Biometrinen tunnistautuminen, Tunnistautumisjärjestelmä, Jatkuva tunnistautuminen.

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Data processing

2019 | 16 pages

Aki-Petteri Koskela

PLAN FOR CONTINUOUS AUTHENTICATION SYSTEM

for a voice controlled management system

The company that commissioned this thesis has a voice controlled management system, that they aim to develop for an authentication system with the purpose of increasing credibility and effectiveness of quality assurance. The purpose of this thesis is to create a plan for the architecture of the authentication system, while choosing technologies to be used in the project. As much of the works as possible is to be completed in the practical part of the work.

Work on the plan was done by the author working for the company developing their software. Purpose of this was to gain an understanding of how the software works and the development needs of the company. Very quickly it became apparent that a multi-modal biometric authentication system would be a perfect solution. The chosen methods of biometric authentication were face recognition and voice biometrics. Alongside them it was decided to implement a PIN-code functionality for additional authentication. The authentication system was design to be modular so that the company can easily implement new authentication technologies and innovations in the future.

A plan for the architecture of the system, along with the chosen technologies for the implementation that were deemed fitting for the needs of the company, was produced during the practical part of the work. Along with the plan, face recognition and pin-code functions were fully implemented. The company will continue the development of the authentication system based on this plan.

KEYWORDS:

Biometrics, Biometric authentication, Authentication system, Continuous authentication

SISÄLTÖ

KUVAT

1 JOHDANTO

Toimeksiantaja yrityksellä on tekoälyyn perustuva ääniohjattu työnohjausjärjestelmä, johon kehitetään kykyä tunnistaa ohjelman käyttäjät kunakin hetkenä. Yritykselle on tärkeää, että tunnistautumisjärjestelmä tulee olemaan joustava, sekä tulevaisuuden varma. Yritykselle on tärkeää, että tunnistautumisjärjestelmä soveltuu

ohjelmiston mahdollisiin tuleviin iteraatioihin mahdollisimman hyvin. Järjestelmän tulee myös olla rakennettu siten että siihen on mahdollista ottaa käyttöön mahdollosia tulevia innovaatioita biometrisen tunnistautumisen puolella.

Voice-user interface eli äänikäyttöliittymät ovat yleistyneet viime vuosina, kun puheentunnistus teknologia on kehittynyt. Ne ovat nousussa etenkin Internet of things laitteiden käyttöliittyminä. Suuret kehittäjät ovat julkaisseet omia äänikäyttöliittymiä hyödyntäviä palveluita, kuten Amazon Alexa ja Google Assistant. Tunnistautumista ei voi näillä laitteilla toteuttaa perinteisesti, sillä niillä ei ole perinteistä graafistakäyttöliittymää, vaan kaikki käyttäjän syöte tapahtuu äänen välityksellä. Tämä luo uusia haasteita, joissa käyttäjä tulee tunnistaa luotettavasti pelkästään äänen perusteella.

Tämän työ tarkoituksena on luoda tunnistautumisjärjestelmän suunnitelma, joka täyttää asiakkaiden laadunvarmistuksen vaatimukset. Suunnitelmassa pyritään luomaan kuva järjestelmän kokonaisarkkitehtuurista sekä valita käytettäviä tunnistautumismenetelmiä ja -teknologioita. Vaikka teknologiat valitaan tässä vaiheessa, järjestelmän tulee olla joustava mahdollisille tuleville innovaatioille.

Suunnitelma toteutetaan työskentelemällä toimeksiantajan ohjelmiston parissa, tarkoituksena on ohjelmiston toimintaan tutustuminen ja sen ymmärtäminen. Sen lisäksi tehdään tutkimusta eri järjestelmäarkkitehtuuresta sekä tunnistautumismenetelmistä ja -teknologioista. Tutkimus tapahtuu keräämällä jo olemassa olevaa tietoa sekä analysoimalla eri artikkeleita ja muuta avointa tietoa aiheista. Tulosten analysoinnissa on tärkeää kuitenkin ottaa huomioon, että tärkeintä lopullisessa suunnitelmassa on sen soveltuvuus yrityksen ohjelmistoon.

Suunnitelman onnistumisessa onkin tärkeintä sen soveltuvuus yrityksen käyttöön. Sitä tutkimaan arvioimalla yrityksen tarpeita ja vertailemalla suunnitelman eri vaiheita yrityksen tarpeisiin. Myös yrityksen tyytyväisyys suunnitelmaan on tärkeä arvioinnissa. Myös yleisiä periaatteita, kuten luotettavuus ja turvallisuus, arvioimalla voidaan tehdä johtopäätöksiä.

Jatkuvan tunnistautumisen äänikäyttöliittymässä on tällä hetkellä kaksi suosittua toteutustapaa. Ensimmäinen vaihtoehto on ottaa puhutusta äänestä sen piirteitä, kuten MFCC (Mel-frequency cepstral coefficent) ja luomalla näistä malli, jonka avulla toteutetaan biometristä tunnistautumista. Toinen vaihtoehto on fyysinen sensori, joka kerää tietoja puhujasta, kuten sijainti ja äänihuulten asento (Feng ym. 2017). Ensimmäinen vaihtoehto sopii tähän käyttötarkoitukseen hyvin, sillä yrityksellä on jo ennestään osaamista koneoppimisen alalta. Tämä toteutus siis soveltuu yrityksen valmiiseen toimintaan. Valittu vaihtoehto ei myöskään vaadi erillistä fyysistä laitetta, mikä tekee siitä taloudellisemman ottaa käyttöön.

2 TUNNISTAUTUMISEN PERIAATTEET

Tässä luvussa tutkitaan tunnistautumiseen liittyvää teoriaa ja miten NIST (National institute of standards and technology) määrittelee siihen liittyvät protokollat. Tarkoituksena on saada ymmärrys näistä periaatteista ennen järjestelmän suunnitteluun siirtymistä.

2.1 Digitaalinen identiteetti

Tunnistautuminen tarkoittaa henkilön digitaalisen identiteetin todentamista. ISO/IEC 24760-1 määrittelee digitaalisen identiteetin ominaisuuksina jotka kuuluvat jollekkin entiteetille (ISO/IEC 24760-1:2019). Entiteetti voi olla henkilö, organisaatio tai laite ja ominaisuuksilla tarkoitetaan järjestelmässä olevaa tietoa joka kuuluu kyseiselle entiteetille. Ominaisuuksiin voi kuulua esimerkiksi käyttäjänimi ja salasana, syntymäaika tai sosiaaliturvatunnus (Technopedia). Sen tarkoituksena on tietokonejärjestelmään tunnistautuminen täysin tietokoneen välityksellä, ilman inhimillistä tekijää. Digitaalinen identiteetti siis sisältää tunnistautumiseen tarvittavaa tietoa.

Entiteetin määritteleminen on vaativaa eikä yksiselitteistä. Yhdellä henkilöllä voi olla monia digitaalisia identiteettejä erilaisissa palveluissa verkossa, esimerkiksi sähköposti ja verkkopankki. Myös yksi laite voi toimi samaanaikaan niin ammattilaisen työkaluna työelämässä, kuin myös median suoratoisto palveluissa. Digitaalinen identiteetti on erillinen oikeanmaailman henkilöllisyydestä. Onnistunut tunnistautuminen on tärkeää, jotta voidaan olettaa palvelua käyttävän henkilön olevan kyseisen palvelun haltia. (NIST 2017.)

2.2 Identiteetin varmistus

NIST (2017) määrittelee digitaalisen identiteetin mallin seuraavasti. Ensimmäisenä tunnistettava entiteetti hakee pääsytietoja tunnistautumisen tarjoalta. Tunnistautumisen tarjoaja varmistaa henkilöllisyyden ja vaihttaa pääsytietoja tunnistettavan kanssa. Tunnistautumisen tarjoajan tulee ylläpitää pääsytietoja vähintään niiden koko voimassaoloajan ja tunnistettavan tulee ylläpitää omat varmenteet, kuten salasana tai avaintunnuskortti. Tämä osa mallista kuvaa pääsytietojen hakemisen ja luovuttamisen.

Malli kuvaa digitaalisen varmennuksen suorittamisen seuraavasti: Ensimmäisenä tunnistettava todistaa hallitsevansa varmennetta tai varmenteita, authetication protokollan läpi. Toiseksi tunnistautumisen tarjoaja validoi pääsytiedot ja yhdistävät henkilöllisyyden varmenteeseen. Kolmanneksi tunnistautumisen tarjoaja tarjoaa lausunnon tunnistautumisesta pyydetylle palvelulle, joka hyväksyy päätöksen. Tunnistautuminen on onnistunut ja kestää istunnon ajan. (NIST 2017.)

3 BIOMETRINEN TUNNISTAUTUMINEN

Biometrinen tunnistautuminen tarkoittaa henkilön automaattista tunnistautumista anatomisten tai käyttäytymiseen perustuvien tuntomerkkien perusteella. Biometrisillä tuntomerkeillä on seuraavia etuja verrattuna perinteisiin käyttäjätunnusten ja salasanojen kaltaiseen valtuutuksiin: niitä ei tarvitse muistaa ja biometrisen datan väärentäminen sekä varastaminen on vaikeampaa.

Biometrisen tunnistautumisen järjestelmä vaatii piirteen, joka on uniikki joka henkilölle ja joka ei muutu lainkaan tai muuttuu hyvin hitaasti. Esimerkiksi: sormenjälki, kasvot tai iiris ovat suosituimpia piirteitä biometrisissä järjestelmissä. Järjestelmät voivat olla voivat olla joko varmistautumis- tai tunnistautumisjärjestelmiä. Varmistautumisjärjestelmä varmistaa onko henkilö kuka hän väittää olevansa, tekemällä biometrisen vertauksen joka palauttaa yksinkertaisen ”kyllä tai ei” vastauksen. Tunnistautumisjärjestelmä toimii ilman henkilön väittämää identiteettiä vertaamalla saatuja piirteitä koko tietokantaan. (Michigan State University Biometrics research group 2009.)

3.1 Multimodaalinen biometrinen järjestelmä

Multimodaalinen biometrinen järjestelmä tarkoittaa järjestelmää, joka hyödyntää useampaa kuin yhtä biometristä piirrettä tunnistautumisessa. Verrattuna unimodaalisiin järjestelmiin jotka käyttävät vain yhtä biometristä piirrettä, multimodaalinen tunnistautuminen on tarkempaa ja luotettavampaa. Unimodaaliset järjestelmät ovat haavoittuvia muuttuviin olosuhteisiin kuten: terveydestä johtuvat syyt tai ympäristön muutokset, joita ovat esimerkiksi käheä ääni tai huono valaistus. Yksittäinen biometrinen piirre on myös haavoittuvaisempi identiteetti varkauksille ja huijaushyökkäyksille. Multimodaalisessa järjestelmässä hyökkääjän tarvitsee saada käsiinsä useampi kuin yksi biometrinen piirre toteuttaakseen hyökkäyksen. Järjestelmä kestää myös paremmin vikatilanteita, koska yhden sensorin hajotessa tai muuten poistuessa toiminnasta, muut järjestelmän sensorit pystyvät silti keräämään tunnistautumiseen vaadittavia piirteitä. (Ho ym. 2006.)

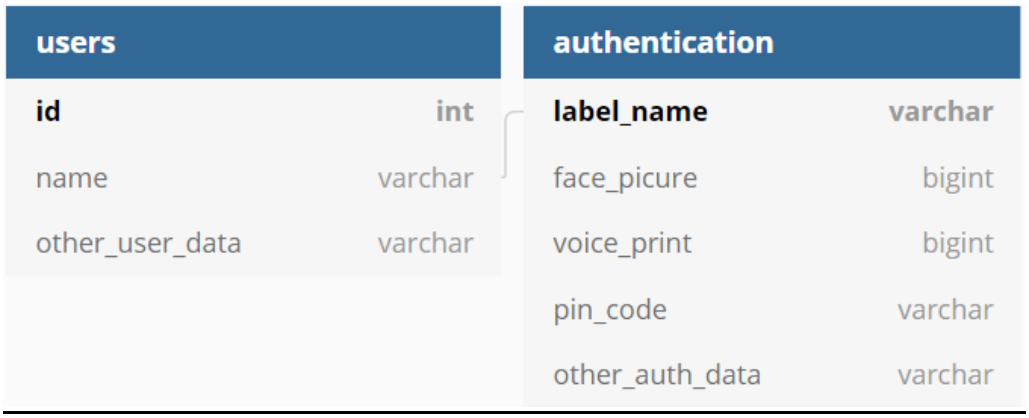
3.2 Toimeksiantajan biometriset järjestelmät

Toimeksiantajan käyttötarkoitus on biometrinen tunnistautumisjärjestelmä, jolla voidaan varmentaa ohjelmiston sen hetkinen käyttäjä. Tämä on tärkeää yritykselle ohjelmiston luotettavuuden ja laadunvarmistuksen näkökulmasta. Yksi ohjelmiston tärkeistä toiminnoista on myös sen helppokäyttöisyys: käyttäjän työnteko ei saa häiriintyä liikaa tunnistautumisesta aiheutuvista toimenpiteistä. Tämän takia toteutukseen valittiin biometrinen järjestelmä, joka voi toteuttaa tunnistautumista työnteon ohessa. Tämä järjestelmä tulee olemaan aikaisemmin mainittu varmistautumisjärjestelmä, joka määrittää onko käyttäjä kuka väittää olevansa. Järjestelmä tulee myös olemaan multimodaalinen järjestelmä, sen aikaisemmin kuvattujen etujen takia.

Kuten monet teknologian alat, biometrisen tunnistautumisen teknologiat kehittyvät hyvin nopeaa tahtia. Odotetulla 18%:n kasvulla aikavälillä 2017–2023, biometrisen teknologian markkinoiden kaikilla biometrisen tunnistautumisen osa-alueilla odotetaan nousevan kolmeenkymmeenkahteen miljardiin dollariin vuoteen 2023 mennessä, sisältäen esimerkiksi: sormenjälki- ja äänitunnistautumisen (Market Research Future 2019). Tämän takia toimeksiantajan järjestelmän tulee olla joustava multimodaalinen järjestelmä, jotta mahdolliset tulevat teknologiat ja innovaatiot on mahdollista ottaa käyttöön järjestelmän nykyisellä arkkitehtuurilla ilman suuria muutoksia tunnistautumisjärjestelmän kokonaisarkkitehtuuriin.

4 TUNNISTAUTUMIS MENETELMÄT

Käytännön osuudessa toteutettiin tunnistautumista seuraavin menetelmin: PIN-koodi, kasvontunnistus ja äänen biometria. Toimeksiantajan vaatimuksesta tunnistautumisjärjestelmän tulee olla käytettävissä erillisenä yrityksen muusta ohjelmistosta. Tunnistautuminen tulee siis toteuttaa joustavalla tavalla, luomalla rajapinnat joihin on helppo päästä käsiksi riippumatta muun ohjelmiston rakenteesta. Toinen tärkeä pointti on tulevaisuus. Jatkossa on mahdollista että toimeksiantaja haluaa lisätä erillaisia tunnistatutumistapoja, joten tunnistautuminen tulee olla rakennettu siten, että niiden integroiminen ja yhteensopivuus mahdollisiin uusiin systeemeihin on helppoa. Tämä on ratkaistu suunnittelemalla tunnistautumisen arkkitehtuuri siten, että kaikki sen osat käyttävät yhteistä käyttäjään sidottua tietoa ja hakevat sen perusteella tietokannasta juuri kyseiseen tunnistautumiseen tarvittavan tiedon (Kuva 1). Tunnistautumiseen tarvittava tieto voi olla esimerkiksi kuva kasvontunnistukseen tai perinteisempi salasana. Seuraavaksi syvennytään valittuihin menetelmiin.



Kuva 1. Tunnistautumiseen tarvittava tieto suhteessa käyttäjään sidottuun tietoon ”label_name”.

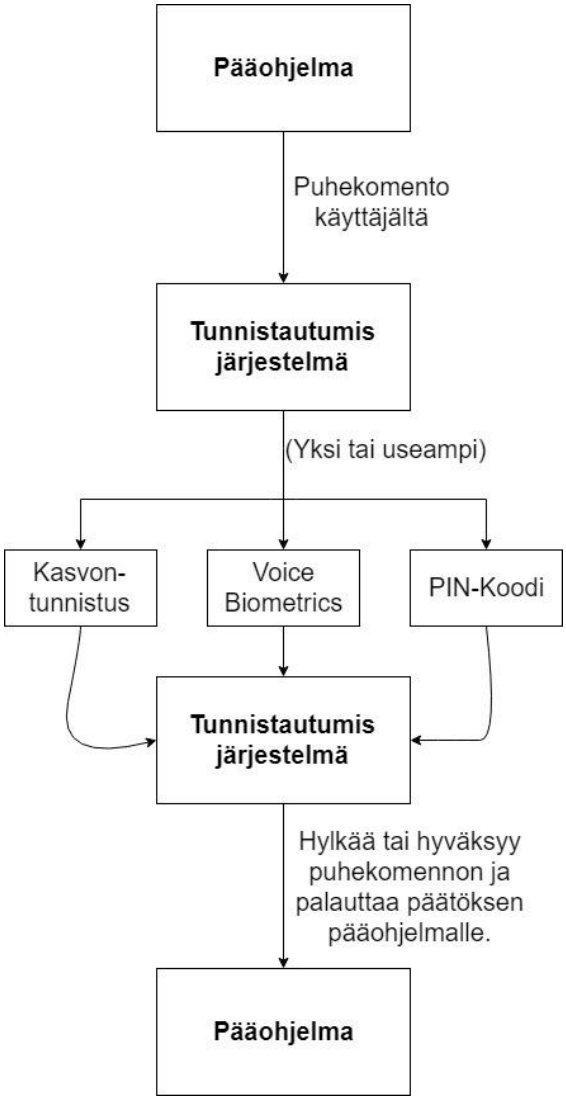
4.1 Kasvontunnistus

Kasvontunnistuksen rooli tunnistautumisen kokonaisuudessa on lisävarmistus ja helppo tunnistautuminen. Lisävarmistuksella tarkoitetaan kaksin- tai kolminkertaista tunnistautumista. Kasvojentunnistus teknologiana on kehittynyt hyvin paljon viime

vuosikymmenen aikana. Teknologia perustuu neuroverkkoon, jota kouluttamalla saadaan koneoppimismalli. Nykyään kasvontunnistusta varten ei kuitenkaan tarvitse kouluttaa omaa ja raskasta mallia, vaan on valmiiksi koulutettuja malleja saatavilla helposti käytteenotettavina kirjastoina eri ohjelmointi kielille.

Käytännönosuudessa kasvontunnistus suunniteltiin ja toteutettiin käyttäen ”Face_Recognition”-kirjastoa Python-ohjelmointikielelle. Se käyttää ”dlib”-koneoppimiskirjaston viimeisintä kasvontunnistusta valmiiseen malliin, jonka voi helposti ottaa käyttöön. Mallilla on 99,38%:n tarkkuus ”Labeled Faces on the Wild” suorituskyky mittauksessa (Geitgey 2019).

Tämän osan toteutus tehtiin luomalla ohjelma, joka lukee tietokannasta tunnistautumistiedon, tässä tapauksessa kuvan, sekä käyttäjän nimen. Kun osaa kutsutaan pääohjelmasta, se lukee webbikamerasta yksittäisen kuvan, tutkii löytyykö kasvoja ja jos kasvot löytyvät, vertaa niitä tietokannasta ladattuihin kasvoihin. Jokaisesta tunnistautumis-yrityksestä luodaan loki merkintä ja tunnistautumisen tulos palautetaan pääohjelmalle, joka voi kutsua kasvontunnistusta uudestaan tai jatkaa ohjelman kulkua (Kuva 2).



Kuva 2. Ohjelman kulku

Kasvontunnistuksella saavutetaan nykyään erittäin hyviä tarkkuuksia, mikä on johtanut kasvontunnistus teknogioiden käytön laajenemiseen. Tämä taas on johtanut erilaisiin kasvontunnistukseen kohdistuviin hyokkäyksiin. On laajalti tunnettu, että kasvontunnistusjärjestelmää pystyy huijaamaan näyttämällä kuvan hyväksytyn henkilön kasvoista. Tämä on kuitenkin helppo torjua ihmisen tarkkailulla: kuka tahansa ympärillä tai valvontakameroissa näkee tämän tapahtuvan. Kasvonmuutoshyökkäykset, jossa käyttäjä koneellisesti yhdistää kahdet kasvot, ovat haastavempia havaita. Ne huijaavat järjestelmää tunnistamaan molemman yhdistetyn kuvan henkilöt ja hyväksyy molempien pääsyn järjestelmään, vaikka vain toinen on oikeasti hyväksytty. Algoritmeja on kehitteillä tunnistamaan tällaiset muokatut kuvat, mutta ne eivät ole vielä täydellisiä. (Scherhag ym. 2017.)

4.2 Äänen biometria

Jokaisella henkilöllä on äänessä uniikkeja piirteitä, joita voidaan käyttää puhujan tunnistamiseen tunnistautumisjärjestelmässä. Neuroverkot ovat yksi onnistuneimmista tavoista toteuttaa puhujan tunnistamisen malleja. Puhujan tunnistamisen voi jakaa kolmeen kategoriaan: puhujan tunnistus, puhujan varmistus ja puhujan diarioiminen. Puhujan tunnistamisessa puhesignaalia käsitellään, tarkoituksena tunnistaa puhuja useista tunnetuista puhujoista. Puhujan varmistuksessa puheen piirteitä verrataan henkilön valmiiksi tunnettuihin puheen piirteisiin, tarkoituksena selvittää onko puhuja henkilö, joka väittää olevansa. Puhujan diariominen on prosessi, jossa puhesignaali segmentoidaan puhujan henkilöllisyyden mukaan. (Irum ym. 2019.)

Kaikki puhujan tunnistaminen sisältää seuraavat vaiheet: koulutus-, kirjautumis- ja arviointivaihe. Koulutusvaiheessa neuroverkkoa koulutetaan olemassa olevalla datalla, että se oppii tunnistamaan puhujan puhesignaalista. Kirjautumisvaiheessa neuroverkolle syötetään puhujien lausumia, jotta saadaan valmis puhujan tunnitamismalli. Arvointi vaiheessa mallia verrataan samanlaisiin olemassaoleviin malleihin ja pohditaan onko lopputulos hyvä vai huono, ja onko se parannettavissa. Puhujan tunnistamis järjestelelmät voidaan jakaa tekstistä riippuviin- ja tekstistä riippumattomiinjärjestelmiin, perustuen kirjautumisvaiheessa käytettyyn dataan. Tekstistä riippuvissa järjestelmissä puhujien lausumat ovat samat kuin kirjautumis- ja arviontivaiheissa, kun taas tekstistä riippumattomattomissa järjestelmissä lausumat voivat vaihdella vapaasti. Nimiensä mukaisesti tekstistä riippuvat järjestelmät vaativat aina saman puhutun lauseen, kun taas tekstistä riippumattomat järjestelmät eivät vaadi tiettyä lausetta tunnistukseen. (Irum ym. 2019.)

Toimeksiantajan ohjelmistossa ei voida ennustaa käyttäjän lausumia kaikissa käyttötapauksissa, joten ensimmäinen puhujan tunnistamisjärjestelmän vaatimus on että sen tulee olla tekstistä riippumaton. Järjestelmän rooli on puhujan varmistus: ei ole tärkeää tietää kuka puhuja on vaan ainoastaan, onko puhuja tunnistautunut käyttäjä. Artikkeli ”Text-independent speaker verification using 3D convolutional neural networks” täyttää molemmat vaatimukset ja tarjoaa avoimen lähdekoodin toteutuksen puhujan tunnistamisen koneoppimismallille. Sen esittämä tarkkuus ja virheprosentti ovat paremmat kuin muiden mallien (Kuva 3). Muitakin puhujan tunnistamisen toteutuksia on, mutta tämä täyttää kaikki vaatimukset avoimella lähdekoodilla ja hyvällä esitetyllä suorituskyvyllä. (Torfi ym. 2018).

representation-level	model	system	EER	AUC
frame [21]	i-vector	-	25.3%	80.5%
frame [13]	LCN	d-vector	24.9%	81.2%
utterance [14]	LCN	d-vector	24.2%	82.6%
utterance [13]	CNN	d-vector	23.9%	83.1%
utterance [14]	LSTM	End-to-End	22.4%	86.0%
utterance [ours]	**3D-CNN**	proposed	**21.1%**	**87.3%**

Kuva 3. Eri puhujan varmistus mallien suorituskyvyt (Torfi ym. 2018).

4.3 PIN-koodi

PIN-Koodi on salainen numerosarja. Se on jo ennestään monille käyttäjille tuttu SIM-kortin lukituksesta tai pankkikortin tunnuslukuna ja täten tarjoaa käyttäjälle tutun tavan parantaa turvallisuutta. Vaikka kyseessä on äänikäyttöliittymä tulee PIN-koodi syöttää graafisenkäyttöliittymän avulla. Numerosarja ei tule olemaan salainen jos käyttäjä puhuu sen ääneen niin, että kuka tahansa ympärillä kuulee sen. Jos graafisenkäyttöliittymän käyttö tapahtuu kosketusnäytöllä, tulee numeroiden järjestyksen olla satunnainen, jotta näytölle ei jää sormenjäljistä tahroja, jotka paljastavat numerosarjan. Syötettyjen numeroiden naamioiminen käyttöliittymässä, esimerkiksi tähdiksi tai palloiksi, on suositeltavaa, etteivät ympäröivät ihmiset vahingossa tai tarkoituksella näe syötettyä numerosarjaa. Käyttäjätilien lukitsemista väärien arvauksien jälkeen ei oteta käyttöön, sillä OWASP:in (The open web application security project) mukaan tämä voi johtaa ongelmiin, joissa hyökkääjä voi estää koko tilin käytön (OWASP). Tämä ongelma on sen sijaan ratkaistu asettamalla PIN-koodin rooli järjestelmään siten, että pelkästään sen murtaminen ei riitä.

PIN-koodin rooli järjestelmän kokonaisuudessa on lisävarmistus käyttäjän määräämissä arkaluontoisissa toiminnoissa sekä muun tunnistautumisen epäonnistuessa. PIN-koodin syöttäminen vaatii käyttäjältä pääsyn ohjelmiston graafiseenkäyttöliittymään, joka on erillinen ohjelmiston tavallisesta äänikäyttöliittymästä. Tämä voi johtaa tilanteisiin missä käyttäjällä ei ole helppoa pääsyä graafiseenkäyttöliittymään. PIN-koodia ei siis voida kysyä liian usein tavallisessa käytössä tai se häiritsee käyttäjän työntekoa, mikä on ohjelmiston tarkoituksen vastaista. PIN-koodin käyttö tapahtuu täten vain kun: käyttäjällä on ylennetyt käyttöoikeudet tai kun kyse on asiakkaan itse määrittelemistä prosesseista.

5 TOTEUTUKSEN HAASTEET

Järjestelmän käytännön toteutukseen liittyy haasteita. On tärkeää olla tietoinen mitä nämä haasteet ovat, jotta ne osataan ottaa huomioon ja siten välttää niistä aiheutuvia ongelmia. Yksi tärkeimmistä tarpeista tunnistautumisjärjestelmälle liittyy laadunvarmistukseen ja sen luotettavuuteen. Toimeksiantaja ei voi ennustaa mitä tarpeita mahdollisilla asiakkailla on noudatettavien standardien ja säännösten suhteen. Tavoitteena on että ohjelmisto täyttää mahdollisimman monet vaatimukset valmiiksi. Esimerkiksi FDA (Food and drug administration) määrää että kaikissa lääkinnällisissä laitteissa pitää huomioida ja ylläpitää kyberturvallisuus ja siihen liittyvät riskit (FDA 2019). Toinen haaste liittyy kerättäviin ja käsiteltäviin henkilötietoihin. Puhujan tunnistamisen mallin kehittäminen vaatii suuria määriä puhedataa, jonka kerääminen ja käsittely tulee olla GDPR:n (General data protection regulation) mukaista.

5.1 Laadunvarmistus ja riskien hallinta

Asiakkailla voi olla prosesseja, joissa on tärkeää olla varma, kuka ollut käyttäjänä eri käyttökertoina. Ehdotettu puhujan tunnistamis järjestelmä tarjoaa kyvyn seurata, kuka käyttää ohjelmistoa, ja täten myös suorittaa prosessia, yksittäisellä komento tasolla tai vaihtoehtoisesti laajemmalla koko prosessin tasolla. Tunnitautumis järjestelmä tulee olla todennettu turvalliseksi, jotta se täyttää mahdolliset asiakkaiden säännökset ja standardit, jotka ottavat kantaa laitteiden kyberturvallisuuteen.

FDA määrittelee että ohjelmiston kehittäjällä on vastuu lääkinällisten laitteiden turvallisuudesta, riskien tunnistamisesta ja mahdollisten korjauksien päivittämisestä. Asetetut vaatimukset riippuvat ohjelmiston kriittisyydestä. Kaikissa ohjelmissa dokumentoitavia asioita ovat: kuvaus järjestelmän toiminnasta, kuvaus järjestelmän käyttöönotosta ja -testauksesta, mahdollisten riskien tunnistaminen ja huomioiminen sekä miten nämä kaikki vaiheet liittyvät toisiinsa. Kaikessa dokumentaatiossa tulee keskittyä mahdollisiin riskeihin ja niiden estämiseen. (FDA 2019.)

Toimeksiantaja pyrkii tunnistamaan ohjelmistoon liittyviä riskejä siten, että ne voidaan huomioida ja niihin vastata. Tunnistautumisjärjestelmälle tämä tarkoittaa, että sen turvallisuutta ja haavoittuvuuksia tulee arvioida, niin kokonaisuutena, kuin yksittäisellä teknologia tasolla. Koko tämän suunnitelman ajan on kuvailtu turvallisuus etuja sekä -

haasteita tehdyille valinnoille. Yrityksen tulee kuitenkin jatkaa ja kehittää turvallisuuden arviointia ja -dokumentointia myös tulevaisuudessa. Ohjelmiston turvallisuuden arvionti ja dokumentointi suositellaan ottamaan osaksi yrityksen tietoturvapolitiikkaa ja ohjelmistonkehitys prosessia.

5.2 Henkilötietojen käsittely

Puhujan tunnistamis järjestelmän kehitys vaatii suuria määriä puhetietoa, joka sisältää äänitiedoston puheesta ja siihen liittyvän metatietoa. Metatieto sisältää tunnisteen, kuka puhuja on, tämän ei tarvitse olla oikea nimi, sekä teksti muodossa mitä äänitiedostossa sanotaan. Puhetietoa kerätään ainoastaan yrityksen omien koneoppimismallien kehittämiseksi. Sitä voidaan kuunnella datan eheyden varmistamiseksi, mutta kuuntelija ei tiedä puhujan henkilöllisyyttä.

Euroopan Unionin tietosuoja-asetus määrittelee kaiken tiedon joka liittyy tunnistettavaan tai tunnistettavissa olevaan henkilöön henkilötiedoksi (Tietosuoja-asetus 2016/679). Puhujan tunnistamisen malli tarvitsee jonkin tunnisteen puhujasta, minkä vuoksi tieto on mahdoton anonymisoida täysin. Sen sijaan tiedot voi säilyttää pseudonymisoituna, mikä tarkoittaa, että niitä ei voida yhdistää henkilöön ilman muualla säilytettävää lisätietoa. Aikaisemman määritelmän mukaan, tämä tarkoittaa, että käsiteltävä tieto on pseudonymisoinnista huolimatta henkilötietoa. Henkilötietoa voi kerätä ja käsitellä, mutta yrityksen tulle olla tietoinen siihen liittyvistä vaatimuksista ja rajoituksista.

Henkilötietoja saa käsitellä jollakin laillisella käsittely perusteella, joka tässä tapauksessa on rekisteröidyn suostumus. Suostumuksen tulee olla yksiselitteinen tahdonilmaisu, joka pitää olla mahdollista perua koska tahansa. Siinä tulee olla selvää mitä tietoja käsitellään ja mihin tarkoitukseen, eli tässä tapauksessa puhetiedon käsittelyä koneoppimismallin kehittämiseen. Yrityksen tulee laatia seloste henkilötietojen käsittelytoimista. Selosteen tulee sisältää: rekisterinpitäjä ja tietosuoja vastaava, käsittelyn tarkoitus, keitä rekisteröidyt ovat ja mitä tietoja käsitellään, luovutetaanko tietoja ja kenelle sekä tietojen säilytysajat. Lisäksi siinä kuvataan yrityksen turvatoimet, kuten käytön rajaus, käytön valvominen ja suojaus ulkopuolisilta. Selosteen tarkoitus on osoittaa että henkilötietojen käsittely on lainmukaista. Henkilötietojen käsittelyyn liittyy informointivelvoite tietojenkäsittelyyn tapahtuvista muutoksista tai ongelmista kuten tietomurroista. (Tietosuoja-asetus 2016/679.)

Koneoppimismallit ovat haastava aihe henkilötietoihin liittyen. Mallien kouluttaminen vaatii suuria määriä tietoa, mutta kun malli on koulutettu se ei enään ole henkilötietoa GDPR:n määritelmän mukaan. Teknisestä näkökulmasta, olemassa olevasta mallista ei voi erottaa tietyn henkilön tietoja, se vaatisi kokonaan uuden mallin kouluttamisen. Tämä estää henkilön oikeuden pääsyn omiin tietoihinsa, sekä oikeuden tulla unohdutetuksi, sillä pääsyä alkuperäiseen tietoon ei ole. Vaikka tiedot saisi poistettua, se tarkoittaa että uudelleen koulutettu malli ei välttämättä suoriudu yhtä hyvin. Ongelmana on mallinkääntämishyökkäys, joka pystyy uudelleen kääntämään valmiin koneoppimis mallin takaisin koulutustiedoksi. Tämä käännetty koulutustieto on jälleen muodossa joka muistuttaa pseudonymisoitua tietoa ja on tapahtunut tietomurto. (Veale ym. 2018.)

Tällä hetkellä GDPR ei pidä koneoppimismallia henkilötietona. Se on kuitenkin murrettavissa ja tällä hetkellä hyvin pinnalla henkilötietosuojaan liittyvissä keskusteluissa. Malleja on hyvä kohdella kuin henkilötietoa: tiukasti määrätty ja rajoitettu tarkoitus ja pääsy niihin tulee olla rajattua. Vaikka laki ei sitä vaadi, tämä on yrityksen edunmukaista sillä vaatimukset voivat hyvin muuttua tulevaisuudessa.

6 LOPPUTULOS JA YHTEENVETO

Tavoitteena tässä työssä oli luoda kattava suunnitelma jatkuvan tunnistautumisen järjestelmästä toimeksiantaja yritykselle. Suunnitelman tarkoituksena oli sisältää tunnistautumisjärjestelmän kokonaisarkkitehtuuri sekä teknologiat, joilla järjestelmän yksittäiset osat toteutetaan. Käytännön osuudessa pyrittiin myös toteuttamaan suunnitelmaa mahdollisimman pitkälle.

Lopputuloksena oli suunnitelma multimodaaliselle biometriselle järjestelmälle, joka käyttää kasvontunnistusta ja äänen biometriaa. Myös uusien teknologioiden integroiminen järjestelmään on mahdollista. Suunnitelma perustuu teoriavaiheessa tehtyyn tutkimukseen erilaisista järjestelmistä ja ymmärrykseen toimeksiantajan toiminnasta ja tarpeista, jotka opittiin tekemällä töitä yrityksellä. Yritys tarjosi hyvin tukea tutkimukselle tarjoamalla aiheeseen liittyvää osaamista ja tutkimusmateriaalia. Tunnistautuminen on jatkuvaa siinä mielessä että jokainen äänikomento voidaan halutessa varmistaa. Yrityksen käyttöön tämä on riittävää, sillä tarkempi seuranta vaatisi lisä sensoreita ja häiritsisi käyttäjien yksityisyyttä. Tällä perusteella ehdotettu ratkaisu on joustava ja yritys voi valita kuinka usein äänikomentoja tulee varmistaa.

Suunnitelmassa on edelleen haasteita liittyen biometristen järjestelmien haavoittuvuuksiin sekä ongelmiin koulutukseen ja tunnistautumiseen vaadittavan tiedon keruussa. Haasteet ovat huomioitu suunnitelmassa käymällä ne lävitse ja ehdottamalla, miten toimia niiden minimoimiseksi. Mikään haasteista ei myöskään ole ylitsepääsemätön, siten että estäisi toteutuksen käyttöönoton. Kunhan yritys huomio haasteiden ratkaisut, järjestelmä sopii hyvin valittuun tarkoitukseen.

Yritys on ilmaissut kiinnostusta jatkaa tunnitautumisjärjestelmän sekä biometristen teknologioiden kehitystyötä, tähän suunnitelmaan perustuen. Suunnitelma täyttää yrityksen vaatimukset modulaarisuudesta ja joustavuudesta. Valittujen teknologioiden tarkkuudet ovat esitetty suunnitelmassa ja ovat multimodaalisesti toteutettuna luotettavat. Järjestelmä nostaa koko ohjelmiston turvallisuutta ja sen teknologioiden haavoittuvuudet ovat huomioitu. Suunnitelmaa voidaan pitää onnistuneena perustuen näiden alussa esitettyjen vaatimusten täyttymiseen sekä yrityksen tyytyväisyyteen.

LÄHTEET

FDA. 2019. FDA's role in medical device cybersecurity. Viitattu 24.11.2019. https://www.fda.gov/medical-devices/digital-health/cybersecurity.

Feng,H; Fawaz,K & Shin,K. 2017. Continuous Authentication for Voice Assistants. Viitattu 25.10.2019 https://rtcl.eecs.umich.edu/wordpress/wp-content/uploads/continuous-authentication-voice.pdf.

Geitgey, A. 2019. Face Recognition. Viitattu 25.10.2019. https://github.com/ageitgey/face_recognition.

Ho,Chiung Ching; Ng, Hu; C, Eswaran. 2006. Survery of approaches and challenges in multi-modal biometric authentication systems. Viitattu 25.10.2019. https://www.researchgate.net/publication/235645116_Survery_of_approaches_and_challenges_in_multimodal_biometric_authentication_systems.

Irum,A; Salman,A. 2019. Speaker verification using deep neural networks: a review. Viitattu 24.11.2019. http://www.ijmlc.org/vol9/760-DT005.pdf.

ISO/IEC 24760-1:2019. IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts. Viitattu 25.10.2019 https://www.iso.org/standard/77582.html.

Market Research Future. 2019. Next generation biometrics market research report – Forecast to 2023. Viitattu 03.11.2019. https://www.marketresearchfuture.com/reports/next-generation-biometrics-market-5955

Michigan State University Biometrics research group. 2009. What is Biometrics? Viitattu 25.10.2019. http://biometrics.cse.msu.edu/info/index.html.

NIST. 2017. Digital Identity Guidelines. Viitattu 25.10.2019. https://pages.nist.gov/800-63-3/sp800-63-3.html#sec4.

OWASP. Päiväämätön. Blocking Brute Force Attacks. Viitattu 20.11.2019. https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks.

Scherhag,U; Raghavendra,R; Raja,K. B; Gomez-Barrero,M; Rathgeb,C; Busch,C. 2017. On the vulnerability of face recognition systems towards morphed face attacks. Viitattu 28.11.2019. https://www.christoph-busch.de/files/Scherhag-VulnerabilityFaceMorphing-IWBF-2017.pdf.

Technopedia. Päiväämätön. What is a digital Identity? Viitattu 25.10.2019. https://www.techopedia.com/definition/23915/digital-identity.

Tietosuoja-asetus. 2016/679, annettu 27.4.2016. Saatavilla http://data.europa.eu/eli/reg/2016/679/2016-05-04.

Torfi,A; Dawson,J; Nasrabadi,N. 2018. Text-independent speaker verification using 3D convolutional neural networks. Viitattu 20.11.2019. https://arxiv.org/pdf/1705.09422.pdf.

Veale,M; Binns,R; Edwards,L. 2018. Algorithms that remember: model inversion attacks and data protection law. Viitattu 28.11.2019. https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0083.